Amendments to the Specification

Page 1, lines 4-10. Please amend the paragraph spanning these lines as follows:

This application is a division of prior application Serial No. 08/884,724, filed June 30, 1997, now U.S. Patent No. 6,339,824, which application is related to the following commonly owned applications, filed concurrently with the prior application and incorporated herein by reference:

R. M. Smith, Sr. et al., "Method and Apparatus for the Secure Transfer of Objects Between Cryptographic Processors", Serial No. 08/885,612, now U.S. Patent No. 6,144,744;

R. M. Smith, Sr. et al., "Method and Apparatus for Controlling the Configuration of a Cryptographic Processor", Serial No. 08/884,721, now U.S. Patent No. 6,108,425.

Page 35. Please amend the Abstract as follows:

Public key security control (PKSC) is provided for a cryptographic module by means of digitally signed communications between the module and one or more authorities with whom it interacts. Authorities interact with the crypto module by means of unsigned queries seeking nonsecret information or signed commands for performing specified operations. Each command signed by an authority also contains a transaction sequence number (TSN), which must match a corresponding number stored by the crypto module for the authority. The TSN for each authority is initially generated randomly and is incremented for each command accepted from that authority. A signature requirement array (SRA) controls the number of signatures required to validate each command type. Upon receiving a signed command from one or more authorities, the SRA is examined to determine whether a required number of authorities permitted to sign the command have signed the command for each signature requirement specification defined for that command type. A command requiring multiple signatures is held in a pending command register (PCR) while awaiting the required cosignatures. The crypto module also stores a single crypto module signature sequence number (CMSSN) which it increments for each reply to any authority

to enable one authority to determine whether any other authority has communicated with the module.